SOLUTION BRIEF

mimecast

Incydr™ + SentinelOne

Contain data risk in response to insider threats

Market Challenges

Insider risk activity poses a complex set of challenges to enterprises. Insider threats, such as malicious insiders or unintentional users with unsecured access, can potentially cause immense financial losses, disrupt operations, and expose confidential data. According to the Annual Data Exposure Report (2022), 71% of businesses lack visibility over what and how much sensitive data departing employees take to other companies. This makes data exfiltration one of the most common types of insider threats, which has only increased with the use of cloud-based collaboration and communication applications. Organizations need an expanded security solution to prevent further exfiltration during insider threat investigations.

Joint Solution

The SentinelOne Singularity XDR and Incydr integration empowers organizations to prevent data exposure and exfiltration. When investigating insider risk alerts in the Incydr console, analysts can quickly respond to data exposure by using SentinelOne's network isolation capability to isolate the user's endpoint to prevent further exfiltration or risky activity.

Together, SentinelOne's best-of-breed XDR technology and Incydr risk monitoring protect organizations from unusual and high-severity activity with the controls to correct and contain data risk.

How It Works

- The integration between Incydr and SentinelOne Singularity XDR can be easily configured via the SentinelOne API with no-code automation services.
- Incydr detects insider risk activity on users' devices and surfaces the threat events for investigation.
- The detected risk activity triggers an automated response via SentinelOne which will quarantine the risky user's device from the network to contain data risk.

Joint Solution Highlights

Exfiltration Detection

Detect and prioritize risk to data to trigger a response via SentinelOne

Network Quarantine

Quarantine the user's device to be unable to access the company's network

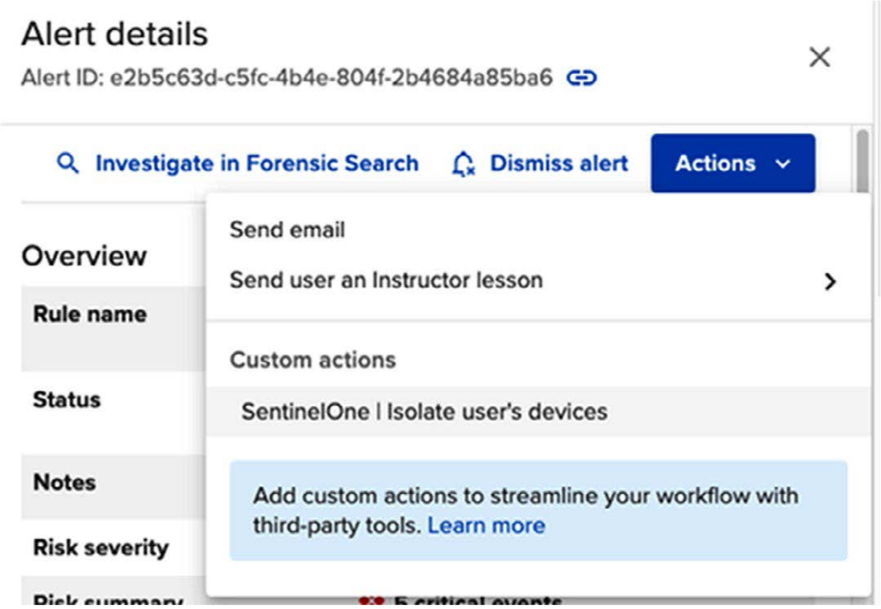
No-code Automation

Easily deploy and manage the integration without additional coding

> "
>
> Data protection is a critical responsibility of every security department. With Incydr and SentinelOne, security teams can quickly detect data exfiltration events and quarantine devices to contain imminent threats.
>
> AIMEE SIMPSON
> DIRECTOR OF PRODUCT MARKETING

Solution Use Cases

Detect and Quarantine – When risky insider threat activity occurs on a user's device, Incydr detects and prioritizes the data risk while SentinelOne quarantines the user's device.



Alert details

Alert ID: e2b5c63d-c5fc-4b4e-804f-2b4684a85ba6

Add custom actions to streamline your workflow with third-party tools. Learn more

Integration Benefits

- Effectively surface the insider threat events that require investigation
- Prevent the user from taking further risky action while you investigate
- Eliminate manual effort by automating device isolation in response to critical events

Conclusion

Together, the SentinelOne Singularity XDR and Mimecast Incydr integration empowers security teams to defend their cyber ecosystem against insider risk with exfiltration detection, automated response, and no-code configuration.

About Mimecast

Mimecast is an AI-powered, API-enabled connected Human Risk Management platform, purpose-built to protect organizations from the spectrum of cyber threats. Integrating cutting-edge technology with human-centric pathways, our platform enhances visibility and provides strategic insight that enables decisive action and empowers businesses to protect their collaborative environments, safeguard their critical data and actively engage employees in reducing risk and enhancing productivity. More than 42,000 businesses worldwide trust Mimecast to help them keep ahead of the ever-evolving threat landscape. From insider risk to external threats, with Mimecast customers get more. More visibility. More insight. More agility. More security.